What is claimed is:

1. A method for providing restricted transmissions of cable modem (CM) configuration files maintained on a trivial file transfer protocol server (TFTP), the method comprising:

using a dynamic host configuration protocol (DHCP) server to associate an un-modified CM configuration filename to a cable modem Internet protocol (IP) address upon receipt of a DHCP REQUEST;

storing a coordination pass phrase on a DHCP server and a TFTP server;

generating a first authentication key;

creating a modified CM configuration filename by combining a CM configuration filename with the authentication key;

transmitting the modified CM configuration filename to the cable modem in a DHCP RESPONSE;

transmitting the modified CM configuration filename from the cable modem to the TFTP server;

parsing the modified CM configuration filename into the un-modified CM configuration filename;

generating a second authentication key;

transmitting the CM configuration file to the cable modem only if the first authentication key matches the second authentication key;

wherein the first authentication key and the second authentication key depend upon the un-modified CM configuration filename, the cable modem IP address and the coordination pass phrase.

2. The method of claim 1 wherein the coordination pass phrase is not known

to the cable modem.

3. The method of claim 1 wherein the first authentication key and the second authentication key are generated using an encryption method selected from the group of methods consisting of block cipher, iterated block cipher, stream cipher, hash function, message authentication codes, factoring, discrete logarithms, elliptic curves, lattice cryptosystems, Data Encryption Standard (DES), Data Encryption Algorithm (DEA), extended Data Encryption Standard (DESX), Advanced Encryption Standard (AES, including MARS, RC6), Digital Signature Algorithm (DSA), Rivest's Cipher (RC2), RC4, RC5, Secure Hash Algorithm (SHA), Message Digest Algorithms (MD2, MD4, MD5), International Data Encryption Algorithm (IDEA), Secure And Fast Encryption Routine (SAFER), Fast Data Encipherment Algorithm (FEAL), Skipjack, Blowfish, Carlisle Adams and Stafford Tavares (CAST) and ElGamal.

4. The method of claim 3 wherein the encryption method is a message digest algorithm.

5. The method of claim 3 wherein the encryption method is the message digest MD5 algorithm.

6. The method of claim 1 wherein the first authentication key further depends upon the cable modem media access control address and wherein the second authentication key further depends upon the cable modem media access control address.

7. The method of claim 1 wherein the coordination pass phrase is generated at random intervals by the DHCP server and transmitted to the TFTP server.

8. The method of claim 1 wherein the coordination pass phrase is generated at random intervals by the TFTP server and transmitted to the DHCP server.

9. The method of claim 7 or claim 8 wherein the random intervals do not exceed an intrusion interval of a wireless network.

10. The method of claim 1 wherein an error message is logged if the first authentication key does not match the second authentication key.

11. The method of claim 1 wherein an error message is generated if the first authentication key does not match the second authentication key and wherein the error message is further transmitted to TFTP server support personnel.

12. The method of claim 1 wherein an alternate cable modem configuration file is transmitted to the cable modem if the first authentication key does not match the second authentication key.

13. The method of claim 12 wherein the alternate cable modem configuration file comprises instructions to disable the cable modem.

14. The method of claim 12 wherein the alternate cable modem configuration file comprises instructions to allow for diagnosing cable modem errors.

15. A method for providing restricted transmissions of cable modem (CM) configuration files maintained on a trivial file transfer protocol server (TFTP), the method comprising:

using a dynamic host configuration protocol (DHCP) server to associate an un-modified CM configuration filename to a cable modem Internet protocol (IP) address upon receipt of a DHCP REQUEST;

storing a coordination pass phrase on a DHCP server and a TFTP server;

generating a first authentication key;

creating a modified CM configuration filename by combining a CM

configuration filename with the authentication key;

creating a cloaked modified CM configuration filename by cloaking the modified CM configuration filename;

transmitting the cloaked modified CM configuration filename to the cable modem in a DHCP RESPONSE;

transmitting the cloaked modified CM configuration filename from the cable modem to the TFTP server;

de-cloaking the cloaked modified CM configuration filename to obtain the modified CM configuration filename;

parsing the modified CM configuration filename into the un-modified CM configuration filename;

generating a second authentication key;

transmitting the CM configuration file to the cable modem only if the first authentication key matches the second authentication key;

wherein the first authentication key and the second authentication key depend upon the un-modified CM configuration filename, the cable modem IP address and the coordination pass phrase.

16. The method of claim 15 wherein the coordination pass phrase is not known to the cable modem.

17. The method of claim 15 wherein the first authentication key and the second authentication key are generated using an encryption method selected from the group of methods consisting of block cipher, iterated block cipher, stream cipher, hash function, message authentication codes, factoring, discrete logarithms, elliptic curves, lattice cryptosystems, Data Encryption Standard (DES), Data Encryption Algorithm (DEA), extended

Data Encryption Standard (DESX), Advanced Encryption Standard (AES, including MARS, RC6), Digital Signature Algorithm (DSA), Rivest's Cipher (RC2), RC4, RC5, Secure Hash Algorithm (SHA), Message Digest Algorithms (MD2, MD4, MD5), International Data Encryption Algorithm (IDEA), Secure And Fast Encryption Routine (SAFER), Fast Data Encipherment Algorithm (FEAL), Skipjack, Blowfish, Carlisle Adams and Stafford Tavares (CAST) and ElGamal.

18. The method of claim 17 wherein the encryption method is a message digest algorithm.

19. The method of claim 17 wherein the encryption method is the message digest MD5 algorithm.

20. The method of claim 15 wherein the first authentication key further depends upon the cable modem media access control address and wherein the second authentication key further depends upon the cable modem media access control address.

21. The method of claim 15 wherein the coordination pass phrase is generated at random intervals by the DHCP server and transmitted to the TFTP server.

22. The method of claim 15 wherein the coordination pass phrase is generated at random intervals by the TFTP server and transmitted to the DHCP server.

23. The method of claim 21 or claim 22 wherein the random intervals do not exceed an intrusion interval of a wireless network.

24. The method of claim 15 wherein an error message is logged if the first authentication key does not match the second authentication key.

25. The method of claim 15 wherein an error message is generated if the first authentication key does not match the second authentication key and

wherein the error message is further transmitted to TFTP server support personnel.

26. The method of claim 15 wherein an alternate cable modem configuration file is transmitted to the cable modem if the first authentication key does not match the second authentication key.

27. The method of claim 26 wherein the alternate cable modem configuration file comprises instructions to disable the cable modem.

28. The method of claim 26 wherein the alternate cable modem configuration file comprises instructions to allow for diagnosing cable modem errors.

29. A method for providing restricted transmissions of cable modem (CM) configuration files maintained on a trivial file transfer protocol server (TFTP), the method comprising:

using a dynamic host configuration protocol (DHCP) server to associate an un-modified CM configuration filename to a cable modem Internet protocol (IP) and a cable modem media access control address upon receipt of a DHCP REQUEST;

storing a coordination pass phrase on a DHCP server and a TFTP server;

generating a first authentication key;

creating a modified CM configuration filename by combining a CM configuration filename with the authentication key;

transmitting the modified CM configuration filename to the cable modem in a DHCP RESPONSE;

transmitting the modified CM configuration filename from the cable modem to the TFTP server;

separately obtaining the cable modem media access control address

associated with the cable modem IP address;

parsing the modified CM configuration filename into the un-modified CM configuration filename;

generating a second authentication key;

transmitting the CM configuration file to the cable modem only if the first authentication key matches the second authentication key;

wherein the first authentication key and the second authentication key depend upon the un-modified CM configuration filename, the cable modem IP address, the coordination pass phrase and the cable modem media access control address.

30. The method of claim 29 wherein the first authentication key and the second authentication key are generated using an encryption method selected from the group of methods consisting of block cipher, iterated block cipher, stream cipher, hash function, message authentication codes, factoring, discrete logarithms, elliptic curves, lattice cryptosystems, Data Encryption Standard (DES), Data Encryption Algorithm (DEA), extended Data Encryption Standard (DESX), Advanced Encryption Standard (AES, including MARS, RC6), Digital Signature Algorithm (DSA), Rivest's Cipher (RC2), RC4, RC5, Secure Hash Algorithm (SHA), Message Digest Algorithms (MD2, MD4, MD5), International Data Encryption Algorithm (IDEA), Secure And Fast Encryption Routine (SAFER), Fast Data Encipherment Algorithm (FEAL), Skipjack, Blowfish, Carlisle Adams and Stafford Tavares (CAST) and ElGamal.

31. The method of claim 30 wherein the encryption method is a message digest algorithm.

32. The method of claim 30 wherein the encryption method is the message digest MD5 algorithm.

33. The method of claim 29 wherein the coordination pass phrase is not known to the cable modem.

34. The method of claim 29 wherein the coordination pass phrase is generated at random intervals by the DHCP server and transmitted to the TFTP server.

35. The method of claim 29 wherein the coordination pass phrase is generated at random intervals by the TFTP server and transmitted to the DHCP server.

36. The method of claim 34 or claim 35 wherein the random intervals do not exceed an intrusion interval of a wireless network.

37. The method of claim 29 wherein an error message is logged if the first authentication key does not match the second authentication key.

38. The method of claim 29 wherein an error message is generated if the first authentication key does not match the second authentication key and wherein the error message is further transmitted to TFTP server support personnel.

39. The method of claim 29 wherein an alternate cable modem configuration file is transmitted to the cable modem if the first authentication key does not match the second authentication key.

40. The method of claim 39 wherein the alternate cable modem configuration file comprises instructions to disable the cable modem.

41. The method of claim 39 wherein the alternate cable modem configuration file comprises instructions to allow for diagnosing cable modem errors.

42. A method for providing restricted transmissions of cable modem (CM) configuration files maintained on a trivial file transfer protocol server (TFTP), the method comprising:

using a dynamic host configuration protocol (DHCP) server to associate an un-modified CM configuration filename to a cable modem Internet protocol (IP) and a cable modem media access control address upon receipt of a DHCP REQUEST;

storing a coordination pass phrase on a DHCP server and a TFTP server;

generating a first authentication key;

creating a modified CM configuration filename by combining a CM configuration filename with the authentication key;

creating a cloaked modified CM configuration filename by cloaking the modified CM configuration filename;

transmitting the cloaked modified CM configuration filename to the cable modem in a DHCP RESPONSE;

transmitting the cloaked modified CM configuration filename from the cable modem to the TFTP server;

separately obtaining the cable modem media access control address associated with the cable modem IP address;

de-cloaking the cloaked modified CM configuration filename to obtain the modified CM configuration filename;

parsing the modified CM configuration filename into the un-modified CM configuration filename;

generating a second authentication key;

transmitting the CM configuration file to the cable modem only if the first authentication key matches the second authentication key;

wherein the first authentication key and the second authentication key

depend upon the un-modified CM configuration filename, the cable modem IP address, the coordination pass phrase and the cable modem media access control address.

43. The method of claim 42 wherein the first authentication key and the second authentication key are generated using an encryption method selected from the group of methods consisting of block cipher, iterated block cipher, stream cipher, hash function, message authentication codes, factoring, discrete logarithms, elliptic curves, lattice cryptosystems, Data Encryption Standard (DES), Data Encryption Algorithm (DEA), extended Data Encryption Standard (DESX), Advanced Encryption Standard (AES, including MARS, RC6), Digital Signature Algorithm (DSA), Rivest's Cipher (RC2), RC4, RC5, Secure Hash Algorithm (SHA), Message Digest Algorithms (MD2, MD4, MD5), International Data Encryption Algorithm (IDEA), Secure And Fast Encryption Routine (SAFER), Fast Data Encipherment Algorithm (FEAL), Skipjack, Blowfish, Carlisle Adams and Stafford Tavares (CAST) and ElGamal.

44. The method of claim 43 wherein the encryption method is a message digest algorithm.

45. The method of claim 43 wherein the encryption method is the message digest MD5 algorithm.

46. The method of claim 42 wherein the coordination pass phrase is not known to the cable modem.

47. The method of claim 42 wherein the coordination pass phrase is generated at random intervals by the DHCP server and transmitted to the TFTP server.

48. The method of claim 42 wherein the coordination pass phrase is generated at random intervals by the TFTP server and transmitted to the DHCP server.

49. The method of claim 47 or claim 48 wherein the random intervals do not exceed an intrusion interval of a wireless network.

50. The method of claim 42 wherein an error message is logged if the first authentication key does not match the second authentication key.

51. The method of claim 42 wherein an error message is generated if the first authentication key does not match the second authentication key and wherein the error message is further transmitted to TFTP server support personnel.

52. The method of claim 42 wherein an alternate cable modem configuration file is transmitted to the cable modem if the first authentication key does not match the second authentication key.

53. The method of claim 52 wherein the alternate cable modem configuration file comprises instructions to disable the cable modem.

54. The method of claim 52 wherein the alternate cable modem configuration file comprises instructions to allow for diagnosing cable modem errors.

55. The method of claim 52 wherein the alternate cable modem configuration file comprises instructions for default network parameter values.